UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FREERKELLY0302@GMAIL.COM; KASHDAGREAT11@GMAIL.COM; TKILBERT17@GMAIL.COM; SEKE.KILBERT@ICLOUD.COM; LILRODAPE@ICLOUD.COM; 786-786-5887 (MARRISSA DIANE WORTHEN); AND 678-873-8509 (CARLOS MENDELL GIPSON) THAT ARE STORED AT PREMISES CONTROLLED BY APPLE, INC. (See attachment A).	Case No. 4:24 MJ 2003 JSD **FILED UNDER SEAL** SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRNOIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Wayne House, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

located in the Northern District of California, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

X evidence of a crime;
X contraband, fruits of crime, or other items illegally possessed;
property designed for use, intended for use, or used in committing a crime;
X a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section		*Offense Description*
Title	Section	
18	2114(a)	Robbery of mail, money, or other property of the United States
18	2114(b)	Possession of property received through robbery
18	1704	Keys or locks stolen or reproduced
18	1708	Thief or receipt of stolen mail matter generally
18	371	Conspiracy

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

✓ Continued on the attached sheet.

❑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury the following is true and correct.

Wayne House Digitally signed by Wayne House Date: 2024.01.26 16:16:42 -06'00'

Applicant's signature

United States Postal Inspector Wayne House
Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: January 29, 2024

Judge's signature

City and State: St. Louis, MO

Honorable Joseph S. Dueker U.S. Magistrate Judge
Printed name and title

AUSA: Torrie J. Schneider

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FREERKELLY0302@GMAIL.COM; KASHDAGREAT11@GMAIL.COM; TKILBERT17@GMAIL.COM; SEKE.KILBERT@ICLOUD.COM; LILRODAPE@ICLOUD.COM; 786-786-5887 (MARRISSA DIANE WORTHEN); AND 678-873-8509 (CARLOS MENDELL GIPSON) THAT ARE STORED AT PREMISES CONTROLLED BY APPLE, INC. (See attachment A).	)	No. 4:24 MJ 2003 JSD **FILED UNDER SEAL** SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRNOIC MEANS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Inspector Wayne House**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 to require Apple, Inc. ("Apple"), an electronic communications service/remote computing service provider, to disclose to the United States records and other information, including the contents of communications, associated with Apple IDs and user identifiers: freerkelly0302@gmail.com; kashdagreat11@gmail.com; tkilbert17@gmail.com; seke.kilbert@icloud.com; lilrodape@icloud.com; 786-786-5887 (Marrissa Diane WORTHEN); and 678-873-8509

(Carlos Mendell GIPSON) that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am an Inspector with the United States Postal Inspection Service ("USPIS") assigned to the St. Louis, Missouri Domicile office and have been since October 2019. I am currently assigned to the Workplace Violence and Security Team, and, in this role, I serve as the Primary Security Inspector and point of contact for lost or stolen Arrow keys. Before this I was assigned to the Contraband Interdiction and Investigation Team and the Financial Investigations Team (previously known as the Mail Fraud Team). Before I was employed with USPIS, I was worked for over sixteen (16) years as a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations in the St. Louis and Kansas City, Missouri field offices, including two (2) years at a Headquarters National Security programmatic unit. I have also worked as a police officer in the City of Chesterfield, Missouri for five (5) years. Throughout my twenty-six (26) year law enforcement career, I have had extensive training, experience, and casework for various criminal violations and investigative categories.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show simply that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that Marrissa WORTHEN, Roderick WALKER, Yahtis BAILEY, Carlos GIPSON, Roderick GAINES Jr., Dontavious COMPTON, Graylen MAYBERRY, and Tommy KILBERT, together with known and unknown persons, have committed violations of Title 18, United States Code, Section 2114(a) (robbery of mail, money, or other property of the United States); Title 18, United States Code, Section 2114(b) (possession of property received through robbery); Title 18, United States Code, Section 1704 (keys or locks stolen or reproduced); Title 18, United States Code, Section 1708 (theft or receipt of stolen mail matter generally); and Title 18, United States Code, Section 371 (conspiracy) ("subject offenses"). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, and fruits of these crimes, as further described in Attachment B.

LOCATION TO BE SEARCHED

5. The locations to be searched are Apple IDs or user identifiers:

- **freerkelly0302@gmail.com**;
- **kashdagreat11@gmail.com**;
- **tkilbert17@gmail.com**;
- **seke.kilbert@icloud.com**;
- **lilrodape@icloud.com**;
- **786-786-5887 (Marissa Diane WORTHEN)**; and
- **678-873-8509 (Carlos Mendell GIPSON)**

("subject accounts") located at a premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California 95014.

BACKGROUND INFORMATION RELATING TO APPLE ID AND iCLOUD[1]

6. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

7. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services and can also be used to store iOS device backups and data associated with third-party apps.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

8. Apple services are accessed using an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

9. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

10. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers.

The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

11. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

12. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly,

the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

13. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for

example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

14. In some cases, account users will communicate directly with Apple about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Apple typically retains records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user because of the communications.

PROBABLE CAUSE

Investigation of Armed Robbery of USPS Carrier

15. On July 20, 2023, USPIS St. Louis was notified of an armed robbery of an Arrow key from a USPS carrier in the area of Chippewa Street and Illinois Avenue, St. Louis, Missouri. This affiant responded to the Maryville Gardens Post Office at 2920 Meramec Street, St. Louis, Missouri, 63118.

16. The victim mail carrier ("Victim Carrier") reported that at approximately 12:10-12:20 p.m. that day, after delivering to 2100 Chippewa Street, which is on the southeast corner of Chippewa Street at Illinois Avenue, he turned to cross the street to continue his route when he was confronted by a dark blue or black four-door sedan with a license plate that began with "PIY" or "P1Y." The vehicle blocked him from crossing the street. The Victim Carrier stated the vehicle was

occupied by three young black males and a young black female who was in the front passenger seat.

17. The driver of the suspect vehicle asked the Victim Carrier if he had "that key." The Victim Carrier, understanding the driver meant an Arrow key, tried to divert and presented his USPS vehicle key, asking if the driver wanted that key. The male on the rear driver's side of the suspect vehicle asked: "where's the key, the key that opens everything" while pointing a dark colored handgun at the Victim Carrier. Simultaneously, the female passenger told the Victim Carrier to "stop playing dumb." Upon seeing the firearm, the Victim Carrier handed the driver of the suspect vehicle the Arrow key. The suspect vehicle then backed up and turned southbound onto Illinois Avenue.

18. The Victim Carrier reported being afraid to call the police because of the neighborhood he was in, as he did not want to be seen talking to police. As such, the Victim Carrier completed his delivery route on the north side of Chippewa Street and returned to his USPS vehicle, which was parked at Chippewa Street and Indiana Avenue.

19. When he returned to his vehicle, the suspect vehicle re-approached him, this time eastbound from Broadway. The Victim Carrier was at the back of his USPS vehicle with the back hatch open, so the occupants of the suspect vehicle could see mail in the back. The driver of the suspect vehicle stated something like: "trying to make sure you not doing that police thing," which the Victim Carrier believed meant he was not calling the police. The driver of the suspect vehicle asked the Victim

Carrier if he had any checks in his USPS vehicle. Wanting to get away, the Victim Carrier gave them an outbound mailing he had just picked up that he believed may contain a check. The occupants of the suspect vehicle asked if he had any more, but the Victim Carrier said he did not. The suspect vehicle left eastbound on Chippewa Street.

20. The Victim Carrier provided descriptions of the occupants of the suspect vehicle:

- Driver: young black male, athletically "bulky" build, light complexion, low-cut black hair, tattoos on both arms, possible tattoo under right eye.
- Front passenger: young black female; light complexion; slim build; tattoos on arms, hands, and thighs.
- Rear driver side: young black male, wearing a hoodie, displayed the firearm.
- Rear passenger side: young black male, wearing a hoodie.

21. This affiant learned that another USPS carrier had been approached in the same general area shortly before the robbery by a similarly described vehicle with four occupants. During an interview, that carrier (Witness Carrier) stated that at approximately 12:00 p.m., he was delivering on foot in the area of 3019 Osage Street when he was approached by a small, black or dark-colored, four-door sedan occupied by three black males and a black female, who was in the front passenger seat. The female passenger asked the Witness Carrier something like: "If I bring a key, what it was good for?" She also asked if it opened "all" the boxes. The Witness Carrier responded that it was only good for boxes in the immediate area and the vehicle drove away. The Witness Carrier did not observe or note the license plate.

22. The Witness Carrier provided descriptions of the occupants of suspect vehicle:

- Driver: black male, early-mid 20's, light-medium brown complexion, low-cut black hair.
- Front passenger: black female, early-mid 20's, light complexion, skinny.
- Rear driver side: black male, early 20's, smaller.
- Rear passenger side: black male, early 20's, a lot of hair (bunched and unkempt).

23. This affiant obtained the series and serial number of the stolen Arrow key (266-59991) and entered it into the National Crime Information Center (NCIC) database as stolen.

24. This affiant also requested the assistance of the St. Louis Metropolitan Police Department's Real Time Crime Center (RTCC) to search available license plate reader (LPR) information and traffic cameras for any vehicles matching the description(s) of the suspect vehicle and bearing a plate starting "PIY" or "P1Y." RTCC located a dark blue Mazda sedan with Georgia license plate PIY2963 that was captured by LPRs and street cameras in or around the south St. Louis area, including the area of the robbery at or near the time of the robbery. Specifically, the vehicle was captured on Broadway at Chippewa Street at approximately 11:53 a.m.

25. Georgia license plate PIY2963 was registered to a Mazda 3 (the Mazda 3) owned by Enterprise Rent-A-Car (Enterprise), 614 Cobb Parkway South, Marietta, Georgia 30060.

26. The Mazda 3 was rented by Marrissa WORTHEN on June 27, 2023, from Enterprise at 3852 Jonesboro Road, Atlanta, Georgia 30354, and was due back on July 18, 2023. WORTHEN provided an address of 336 Triumph (given as Trump) Circle, Atlanta, Georgia 30354. The information listed a contact phone number given at the time of rental as **786-786-5887**.

27. Law enforcement obtained WORTHEN's driver's license photo and a screenshot of her publicly viewable Facebook profile from the Georgia Bureau of Investigation. In the Facebook photo, WORTHEN had numerous tattoos on her arms and legs.

28. Review of further LPR information revealed that the Mazda 3 was in the St. Louis area until at least July 21, 2023. Specifically, it was captured by an LPR at southbound Cross Creek Drive at Olive Boulevard in Creve Coeur, Missouri multiple times on the evenings of both July 20 and 21, 2023. Investigation revealed the presence of both a blue USPS collection box at this location and a large apartment complex.

Enterprise Surveillance Video

29. Enterprise confirmed the return of the Mazda 3 on July 29, 2023. The reported mileage traveled during the rental period was 8,891.

30. Enterprise also provided video footage of the Mazda 3's rental on June 27, 2023. WORTHEN arrived at the rental location in a silver Chevrolet four-door sedan driven by a young black male. WORTHEN walked into the lobby with the black male and they approached the counter together. While at the counter, the black male

lifted the front of his t-shirt, revealing what appeared to be a handgun tucked into the waistband of his pants. After conducting the initial transaction at the counter, WORTHEN and the black male went out to the parking lot with the Enterprise associate, where the black male got into the driver's seat of silver Chevrolet sedan, while WORTHEN got into the driver's seat of the Mazda 3.

31. Inspectors took and enhanced two still images from the Enterprise video and used facial recognition software to identify the young black male who accompanied WORTHEN to pick up the Mazda 3. As a result of facial recognition searches in social media databases, Inspectors obtained possible identifications. Only one social media profile appeared in both results: Roderick WALKER. An open-source database search of "Roderick WALKER" in the Atlanta, Georgia-area revealed a match of Roderick Orlandez WALKER with a previous association with 4360 Yates Road, Atlanta, Georgia 30337.

Ladue, Missouri Mail Theft Investigation

32. On July 27, 2023, the Ladue, Missouri Police Department received a report of mail theft from a USPS blue collection box at 9218 Clayton Road, Ladue, Missouri. According to the police report, a red Ford SUV with Georgia license plates that was occupied by four black males pulled up to the collection box at approximately 10:30 a.m. The driver exited the vehicle, opened the mailbox with a key or tool, and removed mail from collection box, and shoved it down his pants. It appeared that another occupant acted as a lookout. Witnesses also provided a possible Georgia license plate of "SRW5471."

33. Two Ladue LPRs located at different firehouses on Clayton Road captured images of a red Ford SUV with Georgia license plate SCW5471 eastbound on Clayton Road near Dwyer Road at 10:25 a.m., traveling toward the mail theft location, and again at 10:32 a.m. eastbound on Clayton Road at Price Road, traveling away from the mail theft location. These LPRs also captured the vehicle earlier that same day, at 2:26 a.m. and 2:30 a.m. respectively, traveling the same route.

Budget Car Rental Information

34. Georgia license plate SCW5471 is registered to a red Ford Edge (the red Ford Edge) owned by Better Way Leasing, LLC in Marietta, Georgia. Online research of Better Way Leasing revealed it to be a Budget Car Rental (Budget) associated business. Inspectors obtained records associated with the rental of this vehicle during the time of the Ladue mail theft from Budget Security in the Atlanta, Georgia-area.

35. Alexcia Foster (Foster) rented the red Ford Edge on July 25, 2023. Budget also provided still images from its surveillance video at the time of rental, which depicted Foster at the rental counter with a young child and a male who this affiant recognized from the rental of the Mazda 3. Another image depicted the male crouched down next to the red Ford Edge as if he was reviewing the vehicle for damage.

36. Inspectors enhanced the images of Foster and the black male from Budget and, using facial recognition software, identified the same social media accounts for WALKER as with the Enterprise images.

WORTHEN's Phone Number: 786-786-5887

37. On August 18 and August 21, 2023, Inspectors received records from AT&T related to WORTHEN's phone: **786-786-5887**. The subscriber was identified as Ashley Tucker (Tucker), 183 Mount Zion Road, Unit 1102, Atlanta, Georgia 30354, with contact phone number 404-432-5904. It also listed an associated business name of "Rere Ink" at 2798 Peek Road Northwest, apartment 734, Atlanta, Georgia 30039, with a contact number of **786-786-5887**. "Rere Ink" is associated with WORTHEN.

38. An open-source search of "Rere Ink" revealed a possible incorporation in the state of Florida. The Florida Secretary of State's website contains a Florida Profit Corporation registration filing for "Rere Inked, Inc." with WORTHEN listed as a registered agent and President and Tucker listed as the Vice President at 2798 Peek Road, apartment 734, Atlanta, Georgia 30318.

39. AT&T records identified an Apple iPhone 11 with International Mobile Equipment Identity (IMEI) 35685811747017 associated with WORTHEN's phone number. Open-source searches confirmed the IMEI number as an Apple iPhone 11.

Tolls Between WORTHEN, WALKER, and BAILEY

40. Review of WORTHEN's call records revealed high call activity between WORTHEN and phone number 910-631-3903 between June 27, 2023, the day of the Mazda 3 rental, almost daily through July 25, 2023, the day of the red Ford Edge rental.

41. Inspectors sought and obtained records from AT&T for 910-631-3903 and learned that Roderick O. WALKER, 4360 Yates Road, Atlanta, Georgia, was the subscriber with a service start date of November 10, 2022.

42. AT&T records identified an Apple iPhone 12 Pro Max with IMEI 3548765065251 associated with WALKER's phone number in June and July 2023 and an Apple iPhone 13 with IMEI 35493327002352 associated with WALKER's phone number beginning in August 2023. The change in IMEI's indicates WALKER changed devices associated with the account, which corresponds with WALKER's arrest in late-July 2023 in which his cell phone was seized, he remained an Apple customer.

43. WORTHEN's call records also revealed multiple calls with phone number 470-696-8400 on July 19, 2023, the day before the robbery. A search of WALKER's tolls for that number revealed daily call activity between July 12, 2023 and July 27, 2023. According to AT&T subscriber records, the billing party for (470) 696-8400 was listed as Yosaniki Bailey, 7672 Creekside Lane, Riverdale, Georgia as of April 29, 2023, but the user was listed as Yahtis BAILEY.

44. AT&T toll and usage records identified three Apple 14 Pro Max with IMEIs 35063659117192, 35366590865543, and 35854030498613 associated with BAILEY's phone number between late June and early August 2023. The AT&T user information listed an email address of **kashdagreat11@gmail.com**.

Cell Phone Account and Tower Search Warrants

45. This affiant obtained search warrants for both information related to WORTHEN and WALKER's cell phone accounts and cell tower information related to the dates, times, and locations identified in this investigation, including the robbery, mail thefts, and LPR hits. Records received in response showed that WALKER's phone number was captured in all identified locations at the times sought.

46. AT&T records showed WORTHEN in the areas of the Enterprise robbery vehicle rental, the Witness Carrier approach at 3019 Osage Street, the Victim Carrier robbery at 2100 Chippewa, and at Cross Creek and Olive Blvd. between July 20 and July 21, 2023, at the times sought.

47. According to AT&T tower records, 470-696-8400 (BAILEY), was captured on towers in the areas and at the times of the Witness Carrier contact, the Victim Carrier robbery, and the Ladue mail theft.

48. AT&T tower records further identified phone number 470-651-6926 that was captured in the area of the Ladue mail theft and the related LPR captures at 9915 and 9213 Clayton Road. A review of AT&T toll records revealed that 470-651-6926 was in frequent contact with BAILEY from late June 2023 through late July 2023 and with WALKER on July 26, 2023. Through AT&T records, Inspectors identified the subscriber and user of 470-651-6926 as Roderick GAINES, Jr.

49. AT&T records identified an iPhone 13 with IMEI 35570190440950 associated with the phone number. The user information also listed an email address of **lilrodape@icloud.com**.

50. According to T-Mobile tower records, **678-873-8509** was captured on a tower in the area of the robbery on July 20, 2023, when BAILEY called the number at approximately 12:08 p.m. That call also appeared in the AT&T tower records, as the tower to which BAILEY's phone was connected. Searches of BAILEY and WALKER's tolls revealed that **678-873-8509** was in frequent contact with both.

51. An open-source search of **678-873-8509** revealed that it was associated with Carlos GIPSON, whose driver's license lists a home address of 89 Iverness Drive, Jonesboro, Georgia 30328 and a contact phone number of **678-873-8509**. T-Mobile subscriber information lists Kimberly Wise, 89 Iverness Drive, Jonesboro, Georgia 30328 as the subscriber from May 2018 through August 2, 2023,

52. T-Mobile records identified a device with IMEI 350197042891740 associated with the phone number. Open-source research of that IMEI revealed it to be an Apple iPhone 12.

Frontenac, Missouri Mail Theft Investigation

53. On October 12, 2023, the Frontenac, Missouri Police Department (FPD) received a report of a mail theft from the collection box at 10411 Clayton Road, Frontenac, Missouri 63131. A witness reported that two black males in a white Chevrolet Equinox pulled up to the collection box at approximately 3:15 p.m. and a male exited the vehicle, opened the collection box door, and removed mail before

returning to the vehicle, taking the mail with him, and leaving the collection box door open.

54. FPD identified a suspect vehicle from a Frontenac-area LPR that captured a white Chevrolet Equinox (the Equinox) with Georgia license plate SBQ7987 traveling westbound on Clayton Road at Lindbergh Boulevard at approximately 3:10 p.m. that day. Research of Georgia license plate SBQ7987 identified the vehicle as owned by Avis Car Rental (Avis). FPD entered a "wanted-for-investigation" alert for the Equinox and license plate into the NCIC database.

55. On October 13, 2023, FPD notified USPIS of the mail theft and its investigation. It further advised that, if located, it would tow and impound the Equinox.

Avis Car Rental Information

56. On October 13, 2023, Inspectors contacted Avis and learned that the Equinox was rented on September 13, 2023,[2] and was due back September 14, 2023. The renter and sole authorized driver was Jazzmin Greene, 1494 Memorial Drive Southeast, Atlanta, Georgia 30317. Due to its overdue status, Avis provided Inspectors with the Equinox's active GPS data and stated that they wanted the Equinox recovered if law enforcement located it.

57. Using that GPS information, Inspectors located the Equinox parked in front of 5033 Chippewa Street, Saint Louis, Missouri. They began surveillance on it

[2] Inspectors later learned from Avis that the Equinox was actually rented on September 12, 2023.

and observed two black males exit 5033 Chippewa Street and get into the Equinox. One male exited the Equinox and briefly reentered 5033 Chippewa Street before returning to the Equinox. Shortly thereafter, a blue BMW arrived and parked in front of the Equinox. The driver of the BMW got into the Equinox and the three left, traveling to Steak and Shake, 4640 Chippewa Street, St. Louis, Missouri.

58. Given that the Equinox was listed as wanted by FPD and information from Avis that it was an overdue rental, Inspectors, with the assistance of SLMPD and eventually FPD, conducted an investigative stop in the Steak and Shake drive-thru. Inspectors identified the driver as WALKER; the front passenger as Graylen MAYBERRY of Atlanta, Georgia; and the rear passenger as Tommy KILBERT of St. Louis, Missouri.

59. Upon notifying Avis that Inspectors had located the Equinox, Avis provided written consent to search. In the backseat, Inspectors located an M&M wrapper containing a USPS Arrow key, which the Jennings, Missouri Post Office had reported lost between June and July 2023. Elsewhere in the passenger compartment Inspectors located a blue Apple iPhone 13, which WALKER claimed, and a red Apple iPhone 13, which KILBERT claimed.

Interview of KILBERT

60. In an interview, KILBERT stated that he met WALKER, whom he knew as "RJ," in Atlanta through his brother and had only communicated with WALKER via Instagram. KILBERT had not known MAYBERRY before he arrived in St. Louis with WALKER a day or two earlier.

61. In addition to the red iPhone 13, KILBERT admitted that he had another phone in his purse/shoulder bag, which he permitted Inspectors to search and from which they seized a rose-gold Apple iPhone XS Max and two Missouri driver's licenses and eight credit and/or debit cards in other peoples' names.

Investigation at 5033 Chippewa Street

62. Following the stop, Inspectors returned to 5033 Chippewa Street where they were unable to contact anyone at the residence. Law enforcement learned that the property was an AirBnB rental managed by Lage Real Estate, so they contacted a Lage Real Estate representative, who advised that the current renter was Dalvionna Woods of Atlanta, Georgia. After informing the representative of their investigation, Lage Real Estate immediately cancelled the rental, consented to law enforcement's entry onto the property, and provided them with the door code to enter.

63. Inside 5033 Chippewa Street, Inspectors found items consistent with mail theft, including checks in other peoples' names, a book of blank business-style VersaChecks, a red Apple iPhone Mini, and a black Apple MacBook Air laptop.

GPS and LPR Information Relating to the Equinox

64. Further review of the GPS information provided by Avis revealed that on October 12, 2023, the Equinox traveled to the area of the USPS collection box at 9218 Clayton Road—the same collection box that was the subject of the Ladue mail theft. A search of area LPRs revealed multiple images of the Equinox in that area on the afternoon of October 12, 2023.

65. Additional LPR history revealed that the Equinox was captured at southbound Cross Creek at Olive Boulevard in Creve Coeur, Missouri on October 13, 2023. This LPR had also captured both previously-discussed vehicles—the Mazda 3 and red Ford Edge.

Check Fraud Identified

66. FPD identified victims from checks found at 5033 Chippewa Street, including Innovative Claims Service (ICS), a business in Brentwood, Missouri. Specifically, one of the recovered checks was check number 66634, which was originally made payable to Global Claims Service in the amount of $24,383 and mailed to Raleigh, North Carolina.

67. On October 25, 2023, an ICS representative reported to FPD that a check purporting to bear number 66634 had cleared their bank account on October 24, 2023, and that a second check purporting to bear number 66634 was presented for payment but did not clear. ICS reviewed the digital copy of the cleared check and observed that it was made payable to Jacinth Williams, 15925 Northwest 27th Place, Opa Locka, Florida, in the original amount of $24,383. Given that check was physically recovered by Inspectors and the timeframe in which it cleared ICS's bank account, this check forgery likely involved the transmission of a photo of the original check.

Device Search Warrants

68. This affiant obtained a search warrant for the four iPhones and the Apple MacBook Air seized on October 13, 2023. A review of the MacBook Air

extraction revealed a back-up of iMessages from WALKER's phone between June and August 2023. The iMessages were between WALKER and WORTHEN, BAILEY, GIPSON, and GAINES, as well as other unidentified phone numbers.

69. In messaging with WORTHEN (**786-786-5887**), WALKER discussed renting vehicles and swapping out rented vehicles.

70. In messaging with BAILEY (470-696-8400), WALKER and BAILEY discussed washing "slips" with acetone on July 13, 2023, which appears to be a reference to check "washing"—or the physical altering of a check to fraudulently obtain funds from the check writer's account. On July 15, 2023, BAILEY messaged WALKER: "157k slip and the 14k slip I got last night." On July 18, 2023, WALKER sent BAILEY multiple St. Louis area bank location addresses.

71. In messaging with GIPSON (**678-873-8509**), on July 12-13, 2023, WALKER sent addresses of St. Louis-area banks. On July 14, 2023, WALKER sent GIPSON "check out time." On July 16, 2023, GIPSON messaged WALKER that he needed "slips" and asked for "some 5k and a 7k and like some 1k-2k." On July 17, 2023, WALKER stated: "Finan swap rental and get u." Between July 18 and July 20, 2023, WALKER sent GIPSON multiple St. Louis-area bank locations with instructions to go to them. These conversations indicate GIPSON was in St. Louis with WALKER on multiple occasions in July 2023.

72. On July 26, 2023, WALKER messaged 470-997-7056, an unidentified number, and instructed the user to book a St. Louis-area AirBnB. Shortly thereafter,

WALKER messaged GAINES (470-651-6926) and provided him with the unidentified phone number 470-997-7056. There was nothing else included with the message.

73. A forensic extraction of WALKER's blue iPhone 13 revealed that number 910-631-3903 was registered to it at the time of seizure had IMEI 3549332700235216. Walker's registered Apple ID was identified as **freerkelly0302@gmail.com**.

74. The review also revealed photos of checks and identification documents in other peoples' and businesses' names and addresses from across the United States, including Georgia, Louisiana, Pennsylvania, and the St. Louis metro area. A photo of a hand at the keyboard of an Apple MacBook Air while a check was displayed on a Photoshop program was located on WALKER's phone. His phone also contained screenshots of Apple Cash payments, vehicle rental details, AirBnB lodging confirmations, and photos of bulk mail.

75. Forensic extractions of Kilbert's phones revealed a registered Apple ID of **tkilbert17@gmail.com** to the red iPhone 13 and **seke.kilbert@icloud.com** registered to the rose-gold iPhone XS Max.

Preservation Request

76. This affiant sent preservation requests to Apple on January 18, 2024 and January 22, 2024.

77. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the accounts of the Apple users described above. The stored communications and files connected to an Apple ID may provide direct evidence of

the offenses under investigation. Instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

78. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. Subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

79. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information to conceal evidence from law enforcement).

80. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar

information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

81. Therefore, Apple's servers are likely to contain stored electronic communications, photos of evidence (mail, checks, screenshots of transactions) or co-conspirators, videos of criminal activity, location data, illicit financial transaction information, and other information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

82. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the United States copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION AND REQUEST FOR SEALING

83. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United

States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

84. Under 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on AT&T. Because the warrant will be served on AT&T, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

85. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

86. Based on the foregoing, there is probable cause to believe that Marrissa WORTHEN, Roderick WALKER, Yahtis BAILEY, Carlos GIPSON, Roderick GAINES Jr., Dontavious COMPTON, Graylen MAYBERRY, and Tommy KILBERT, together with known and unknown persons, committed violations of Title 18, United States Code, Section 2114(a) (robbery of mail, money, or other property of the United States); Title 18, United States Code, Section 2114(b) (possession of property received

through robbery); Title 18, United States Code, Section 1704 (keys or locks stolen or reproduced); Title 18, United States Code, Section 1708 (theft or receipt of stolen mail matter generally); and Title 18, United States Code, Section 371 (conspiracy), and the subject numbers contain evidence, instrumentalities, and fruits of those violations. The requested warrant will assist law enforcement in its investigation of the subject offenses, and I request that the Court issue the proposed search warrant.

I state under the penalty the perjury the foregoing is true and correct.

Respectfully Submitted,

Wayne House Digitally signed by Wayne House Date: 2024.01.26 16:17:15 -06'00'

Wayne House, Inspector
United States Postal Inspection Service

Subscribed and Sworn to before me via reliable electronic means under Federal Rules and Procedure 4.1 and 41, this 29th day of January, 2024.

HONORABLE JOSEPH S. DUEKER
UNITED STATES MAGISTRATE JUDGE
EASTERN DIISTRICT OF MISSOURI

ATTACHMENT A
4:24 MJ 2003 JSD

Property to Be Searched

This warrant applies to information associated with Apple ID and user identifiers: **freerkelly0302@gmail.com; kashdagreat11@gmail.com; tkilbert17@gmail.com; seke.kilbert@icloud.com; lilrodape@icloud.com; 786-786-5887 (Marisssa Diane WORTHEN);** and **678-873-8509 (Carlos Mendell GIPSON)** ("subject accounts") that are stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT B
4:24 MJ 2003 JSD

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control

("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account **from June 27, 2023 through October 13, 2023**, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account **from June 27, 2023 through October 13, 2023**, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.

II. Information to be seized by the United States

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Section 2114(a) (robbery of mail, money, or other property of the United States); Title 18, United States Code, Section 2114(b) (possession of property received through robbery); Title 18, United States Code, Section 1704 (keys or locks stolen or reproduced); Title 18, United States Code, Section 1708 (theft or receipt of stolen mail matter generally); and Title 18, United States Code, Section 371 (conspiracy) during the period **June 27, 2023 through October 13, 2023.**

a. Evidence of communications between and among WORTHEN, WALKER, BAILEY, GIPSON, GAINES, COMPTON, MAYBERRY, and KILBERT, and others known and unknown, relating to the Subject offenses;

b. Location information;

c. Evidence of travel between Georgia and Missouri, or other states, including but not limited to, contacts with Georgia residents and businesses, accommodation reservations in or en route to or from Georgia and Missouri, or other states;

d. Evidence relating to WORTHEN, WALKER, BAILEY, GIPSON, GAINES, and/or KILBERT's acquisition or possession of Arrow keys; mail, access device cards, or other identification documents in other persons' names;

e. Photographs, videos, messages, and documents relating to the commission of the Subject offenses;

f. Evidence of Internet and mobile application activity, including Internet Protocol addresses, caches, browser history and cookies, bookmarked webpages, search terms, stored passwords, or user-typed web addresses relating to the Subject offenses;

g. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

h. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

i. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

j. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

k. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Apple**, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of **Apple**. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of **Apple**, and they were made by **Apple** as a regular practice; and

b. such records were generated by **Apple's** electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of **Apple** in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **Apple**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature